Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 354

VERSLAG VAN EEN ALGEMEEN OVERLEG
Vastgesteld 5 maart 2015

De vaste commissie voor Veiligheid en Justitie heeft op 22 januari 2015 overleg gevoerd met Minister Opstelten van Veiligheid en Justitie over:
– **de brief van de Minister van Veiligheid en Justitie d.d. 7 juli 2014 inzake Aanpak van botnets (Kamerstuk 26 643, nr. 320);**
– **de brief van de Minister van Veiligheid en Justitie d.d. 10 juli 2014 inzake Beleidsreactie Cyber Security Beeld Nederland 4 (Kamerstuk 26 643, nr. 322);**
– **de brief van de Minister van Veiligheid en Justitie d.d. 13 oktober 2014 inzake Acties omtrent de dataset Hold Security (Kamerstuk 26 643, nr. 328);**
– **de brief van de Minister van Veiligheid en Justitie d.d. 24 november 2014 inzake Verkenning naar de haalbaarheid en wenselijkheid van een gescheiden ICT-netwerk voor (publieke en private) vitale processen (Kamerstuk 26 643, nr. 337);**
– **de brief van de Minister van Veiligheid en Justitie d.d. 18 december 2014 inzake Voortgangsbrief realisatie werkprogramma Nationale Cyber Security Strategie 2 (Kamerstuk 26 643, nr. 341);**
– **de brief van de Minister van Veiligheid en Justitie d.d. 18 december 2014 inzake Voortgang responsible disclosure (Kamerstuk 26 643, nr. 342).**

Van dit overleg brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Ypma

De griffier van de vaste commissie voor Veiligheid en Justitie,
Hessing-Puts

kst-26643-354
ISSN 0921 - 7371
'’s-Gravenhage 2015

Voorzitter: Verhoeven
Griffier: Vermeer

Aanwezig zijn vier leden der Kamer, te weten: Gesthuizen, Oosenbrug, Tellegen, Verhoeven,

en Minister Opstelten van Veiligheid en Justitie, die vergezeld is van enkele ambtenaren van zijn ministerie.

Aanvang 14.00 uur.

De **voorzitter**: Ik heet de Minister en zijn staf van harte welkom bij dit algemeen overleg, net als het publiek dat hier aanwezig is of thuis meekijkt. Uiteraard heet ik ook de collega's van de verschillende fracties welkom. We hebben afgesproken een spreektijd van vijf minuten aan te houden. Gezien het aantal woordvoerders sta ik een uitloop naar zes minuten toe, maar we gaan de tijd natuurlijk niet vol praten.

Mevrouw **Tellegen** (VVD): Voorzitter. IS die social media accounts van de US Central Command hackt en Noord-Korea dat inbreekt in de servers van Sony Pictures. Dat klinkt als een ver-van-mijn-bedshow maar morgen kan Nederland het doelwit zijn van een cyberaanval. We zouden volstrekt naïef zijn als we ons in Nederland voor deze vormen van cybercriminaliteit veilig zouden wanen. Wie van ons heeft het niet al een keer meegemaakt? Je computer loopt vast als gevolg van een virus. Een e-mail van de bank met een waarschuwing om een bepaalde e-mail niet te openen. Een bericht dat je credit card halsoverkop vervangen dient te worden omdat die gehackt is. In welke vorm cybercriminaliteit zich ook voordoet, en of nu een nietsvermoedende burger, de overheid of een ondernemer het slachtoffer is, het is van groot belang dat we werk maken van een veilige digitale samenleving. Daarom kan het beleid om aan cybercriminaliteit het hoofd te bieden, niet genoeg aandacht krijgen.
Het Cyber Security Beeld Nederland geeft ons inzicht in welke digitale belangen we moeten beschermen, vanuit welke hoek de grootste dreigingen komen en op welke punten onze digitale samenleving het kwetsbaarst is. De conclusies stemmen niet al te optimistisch. Het dreigingsbeeld blijft onveranderd en zet zich voort. De impact van cyberaanvallen en verstoringen neemt toe door de snelle digitalisering. Het gebrek aan duurzame ICT-infrastructuur vormt een risico voor de maatschappelijke veiligheid. De dreiging die uitgaat van cybercriminelen blijft onverminderd groot. De Minister beschrijft in zijn brief dan ook terecht de noodzaak tot een integrale, publiek-private en internationale cyber securityaanpak.
Laat ik die drie aspecten er even kort uitlichten. «Een integrale aanpak» is een mooie en vaak gehoorde term. We nemen veel goede initiatieven die erop gericht zijn om de digitale samenleving in Nederland te beschermen. Denk aan het Team High Tech Crime (THTC) van de Nationale Politie. Denk aan het Nationaal Detectie Netwerk, het Nationaal Respons Netwerk, de Cyber Security Raad (CSR), de Abuse Information Exchange en de publiek-private botnetwerkgroep. Het Nationaal Cyber Security Centrum (NCSC) coördineert al deze activiteiten. Kan de Minister aangeven hoe dit gaat? Op rijksniveau zijn er maar liefst vier ministeries met cyber security bezig. Stel je voor dat er een grote digitale aanval plaatsvindt op een elektriciteitsvoorziening in Nederland. Is dan voldoende helder wie waarover gaat? Kortom, kan de Minister aangeven in hoeverre er nu sprake is van een integrale aanpak? Waar zijn er in dit kader nog verbeteringen mogelijk?
Dan kom ik op de publiek-private aanpak. Graag zou ik de Minister willen vragen in welke mate deze samenwerking kan worden versterkt. Het Nationaal Cyber Security Centrum gaat over publiek-private partnerships.

Wat is hier tot nu toe bereikt? In het Verenigd Koninkrijk bestaat een interessant systeem van certificering. Er is een lijst met namen van private instellingen die als vertrouwensbedrijven worden aangeduid en met wie data kunnen worden gedeeld en wier expertise kan worden ingehuurd. Hoe kijkt de Minister hiertegen aan? Zou dat voor Nederland ook een optie zijn?
Dan kom ik op de internationale aanpak. Iedereen weet het: het internet als ecosysteem is van nature grensoverschrijdend en open van karakter. Nederland is gebaat bij een vrij en toegankelijk cyberdomein, maar dat vergt heel nauwe internationale samenwerking. Dat is vooral het geval bij cyberspionage, hacken en bescherming van de vitale infrastructuur. In april dit jaar vindt er in Nederland een grote conferentie plaats. Het is een goede zaak dat Nederland gastheer is van zo'n conferentie. Wat wordt de eigen Nederlandse inzet op deze conferentie?
Bij cybercriminaliteit hebben we het ook over de eigen verantwoordelijkheid van individuele gebruikers. Ieder van ons moet ervoor zorgen dat zijn of haar computer goed beveiligd is. Zo voorkom je dat mensen meekijken met je foto's of misbruik maken van je iDeal. Dit vergt wel dat mensen, bedrijven en ondernemers goed zijn geïnformeerd. Is de Minister van plan de publiekscampagne Alert Online verder door te zetten?
Binnenkort komt het Wetsvoorstel computercriminaliteit III naar de Tweede Kamer. Het doel daarvan is de politie meer slagkracht te geven op het internet, criminelen op het web beter op te kunnen sporen en aan te kunnen pakken. Dat vind de VVD van belang en we wachten dat wetsvoorstel af, maar kan de Minister vandaag al aangeven hoe het Team High Tech Crime van de politie, dat sinds 2012 is ingesteld, werkt en wat de eerste resultaten zijn?

Mevrouw **Oosenbrug** (PvdA): Ik hoor mijn collega zeggen dat het heel belangrijk is dat de consument en de burger zelf goed hun computer beschermen. Binnenkort komt het Wetsvoorstel computercriminaliteit III. Daar zijn wij heel kritisch op omdat een van de aspecten daarvan is dat iemands computer juist onveilig gemaakt kan worden. Hoe kijkt de VVD tegen deze twee aspecten aan, als je ze naast elkaar legt?

Mevrouw **Tellegen** (VVD): Daar zit natuurlijk een spanningsveld tussen. Aan de ene kant gaat het er primair om dat iedereen met een computer thuis verantwoordelijk is voor de veiligheid van zijn eigen computer achter zijn eigen voordeur. Het kan echter van belang zijn dat we onder bepaalde omstandigheden verder gaan als er aanleiding is om in te breken in die computers. Dat is elke keer op nieuw weer iets om zorgvuldig af te wegen.

Mevrouw **Oosenbrug** (PvdA): Het is een zorgvuldige afweging, maar als je computer onveilig wordt gemaakt, waardoor je die verantwoordelijkheid niet meer zelf kunt nemen en je computer onderdeel uit kan gaan maken van een botnet, omdat er kwetsbaarheid op geplaatst is, waar ligt de verantwoordelijkheid voor die computer dan eigenlijk? Kun je die verantwoordelijkheid dan nog wel bij de burger zelf leggen? Ik spar daar zelf ook heel erg mee. Moet er dus een publiek-private samenwerking zijn en moet de burger ook zijn verantwoordelijkheid nemen?

Mevrouw **Tellegen** (VVD): Ik ken de inhoud van het wetsvoorstel dat nog naar de Kamer moet komen niet van voor tot achter, maar het lijkt me dat er dan sprake is van een gedeelde verantwoordelijkheid. Als er besloten wordt om vanwege een gefundeerde reden een computer open te breken, dan is op dat moment zowel de burger als degene die de aanleiding ziet om die computer open te breken verantwoordelijk.
Tot slot kom ik op de motie-Hennis, die oproept tot een wettelijke meldplicht voor zogeheten security breaches. De VVD had die wet al

graag in de Tweede Kamer gezien. In de motie van oud-collega Hennis wordt de regering opgeroepen tot een wettelijke meldplicht. Dat heeft geleid tot de Wet melding inbreuken elektronische informatiesystemen. De motie stamt uit 2011 en nog altijd bestaat er geen plicht voor bedrijven en instellingen om een ontdekking van een digitale inbraak te melden. Graag krijg ik hierop een reactie van de Minister.

Voorzitter: Gesthuizen

De heer **Verhoeven** (D66): Ik weet dat mevrouw Tellegen dit dossier overneemt, maar omdat ik denk dat zij zich goed heeft voorbereid, vraag ik het toch. Die meldplicht vindt D66 ook een heel belangrijk voorstel van de VVD. Voormalig Kamerlid Hennis kwam met dit uitstekende voorstel, maar het kabinet heeft dat voorstel een eind afgezwakt waardoor de meldplicht eigenlijk een beetje een wassen neus lijkt te worden. Het is eigenlijk een meldplicht van niks, een meldplicht die alleen bij zeer groot gevaar in werking treedt. Zou de VVD iets willen zeggen over het gewicht dat zij aan die meldplicht wil geven? Moet dat geen meldplicht zijn die voor alle inbraken geldt en niet alleen voor hele zware?

Mevrouw **Tellegen** (VVD): Ja, met het voorbehoud dat ik niet degene zal zijn die dat wetsvoorstel namens onze fractie zal behandelen. Die motie is destijds niet zomaar ingediend. Het ging erom dat die meldplicht inderdaad een bepaald gewicht moet hebben. Ik kan nu moeilijk aangeven tot in welke mate, maar we zullen zeker bekijken of het geen wassen neus is, want dan lijkt het me een zinloos wetsvoorstel.

De heer **Verhoeven** (D66): Ik ben blij met deze reactie. Ik hoop dat de VVD echt nog eens goed wil nadenken over haar positie ten opzichte van het kabinetsvoorstel. De D66-fractie vindt het in ieder geval nogal mager.

Voorzitter: Verhoeven

De **voorzitter**: Ik wilde trouwens nog zeggen dat we twee interrupties hanteren.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Internet heeft zich de afgelopen 25 jaar uit vrijwel niets ontwikkeld tot de belangrijkste communicatiestructuur ter wereld. Dagelijks maken miljarden burgers, talloze bedrijven en alle overheden hier gebruik van. Ze zoeken of verschaffen informatie, ze bankieren, ze kopen en verkopen, en communiceren, onder andere via social media. In een tijd waarin de afhankelijkheid van digitale communicatienetwerken zeer groot is en alleen maar verder toeneemt, is de betrouwbaarheid van de techniek steeds belangrijker. Tegelijkertijd wordt die betrouwbaarheid bedreigd vanuit diverse hoeken. Het is belangrijk dat Nederland zijn best doet om de kwetsbaarheden in de digitale infrastructuur te verhelpen en daarvoor in internationaal verband samen te werken. Daarin kunnen we onze unieke kwaliteiten inzetten als klein land met een uitstekende digitale infrastructuur en een traditie in diplomatie. Veel van de onveiligheid op internet is niet het gevolg van onvolkomen techniek, maar wordt moedwillig veroorzaakt. Het vertrouwen in de mensen die van dag tot dag internet veilig moeten houden, lijkt onherstelbaar beschadigd. Zo worden beveiligingsupdates van bijvoorbeeld Microsoft soms gebruikt om het mogelijk te maken systemen te hacken. Het gezond en up-to-date houden van hard- en software vormt nu in zichzelf een beveiligingsgevaar. Amerikaanse veiligheidsdiensten hebben sinds 2007 140.000 botnets gekopieerd om mee te liften met cybercriminelen. Wereldwijd zijn 100.000 internetrouters op kritieke netwerken alvast gehackt om later surveillancemogelijkheden te maken. Of, zoals Axel Arnbak heel helder stelt: het vertrouwen in de collectieve hallucinatie die

internet was, is absoluut ondermijnd. Internet is een volstrekte surveillance-omgeving geworden. Vraag is hoe hier tegenwicht aan geboden kan worden. Graag hoor ik van de Minister hoe hij hiertegen aankijkt.
Uiteraard heb ik hier zelf ook nog wel wat over te zeggen. Als klein land denk ik dat we bescheiden moeten zijn in het overschatten van onze capaciteiten om aan offensieve digitale oorlogsvoering te doen. Bovendien is het maar de vraag of we de wereld een dienst bewijzen met deze ondermijning van het internet, waarvan ik zojuist al het belang heb geschetst. Ik denk dat we een heilloze weg opgaan als we meegaan in de lokroep van actief gebruik van de zwakheden in informatiesystemen, alleen al omdat deze kwetsbaarheden zich net zo hard tegen ons kunnen keren. Om het vertrouwen in internet in stand te houden en te verbeteren, is het van belang dat we de keuze maken om de zwakheden gezamenlijk aan te pakken, gekoppeld aan goede wetgeving die veilig en passend gebruik van internet mogelijk maakt.
Uit de stukken die we gekregen hebben, blijkt dat er een herijking is geweest van de vitale infrastructuur. Ik heb al eerder aangegeven dat ik vind dat centrale delen van de internetinfrastructuur vanwege hun belang als vitale infrastructuur aangemerkt zouden moeten worden. Daarnaast is IT een belangrijk instrument voor veel andere vitale infrastructuur. Daarom hoor ik graag van de Minister welke wijzigingen er naar aanleiding van de herijking zijn aangebracht.
De Minister heeft de resultaten gestuurd van een onderzoek naar de haalbaarheid van een gescheiden netwerk voor bijvoorbeeld belangrijke overheidscommunicatie. Alle experts zijn het erover eens dat volledige scheiding feitelijk onmogelijk is en ook in strijd is met het kenmerk van internet. De experts van SURFnet hebben echter wel gewezen op een aantal manieren om het verkeer te scheiden die niet in het onderzoek worden genoemd. Dan gaat het om eigen glasvezel- of lichtpaden. Waarom zijn deze technieken niet meegenomen? Ziet de Minister hier nog mogelijkheden in? Verder wordt er gesproken over de mogelijkheid om delen van het netwerk in eigen beheer te houden. Wanneer gaat de Minister deze mogelijkheden verder uitwerken en hier keuzes in maken?
Een andere zeer concrete actie die genomen wordt op het gebied van cyber security is de aanpak van botnets. Ten aanzien van de gevolgen van een ddos-aanval wil ik vragen hoe de Minister aankijkt tegen de apparatuur die voor kleine internetbedrijven beschikbaar is om deze aanvallen het hoofd te bieden in de vorm van een nationale wasstraat tegen ddos-aanvallen, kortweg de NaWas genoemd. Ziet de Minister heil in het delen van dure apparatuur die de veiligheid op internet vergroot? Welke faciliterende rol neemt de regering hierin?
Daarnaast is er AbuseHUB, waarin het overgrote deel van de isp's informatie met computers uitwisselt. Is de Minister van mening dat isp's nu alles doen om het aantal besmette computers en de gevolgen daarvan terug te dringen? Zo nee, welke acties kunnen er nog meer genomen worden zonder de privacy van gebruikers verder aan te tasten?

De **voorzitter**: U hebt nog één minuut, en dan zit u al in blessuretijd.

Mevrouw **Oosenbrug** (PvdA): De brief over responsible disclosure gaat al bijna meteen de mist in door het te hebben over goedwillende melders of hackers. Alsof dat altijd een tegenstelling is. Ik heb de Minister al meerdere keren proberen uit te leggen dat ook hackers goedwillende melders kunnen zijn. Natuurlijk geldt dat niet in alle gevallen, maar het is stigmatiserend om te ontkennen dat het samen kan gaan. Daarom maak ik dit punt graag nog een keer. Verder geeft de Minister aan dat het OM geen vervolging heeft ingesteld bij de melders die zich aan de richtlijn voor responsible disclosure hebben gehouden van de betrokken organisatie. Ik vind echter dat goedwillende en zorgvuldige hackers zich ook geen zorgen

hoeven te maken over vervolging als er geen responsibledisclosurebeleid is. Graag hoor ik van de Minister welke mogelijkheden hij hiervoor ziet.
Ten slotte de aanwezigheid van de politie op internet: een onmisbare schakel voor een goede aanpak van cyber security. Zo is er het Landelijk Meldpunt Internetoplichting van de politie. Dat is een mooie en belangrijke faciliteit om de handel op internet eerlijker en betrouwbaarder te maken. Dit meldpunt moet geïntegreerd worden in de Nationale Politie, inclusief de ondersteunende systemen die speciaal voor dit meldpunt ontwikkeld zijn. Dit alles zou moeten gebeuren met ingang van 1 maart. Ik heb echter duidelijke signalen ontvangen dat deze deadline niet gehaald gaat worden, waardoor deze dienstverlening van de politie zou stoppen.

De **voorzitter**: Kunt u afronden?

Mevrouw **Oosenbrug** (PvdA): Kan de Minister garanderen dat het Landelijk Meldpunt Internetoplichting soepel door blijft draaien? Zorgt de Minister ervoor dat de bijbehorende informatiesystemen ook gebruikt kunnen blijven worden? Deelt hij mijn mening dat een meldpunt internetoplichting bij de politie een belangrijke bijdrage levert aan de cybersecuritystrategie en dat het behouden moet blijven?

De **voorzitter**: Dan is nu het woord aan mevrouw Gesthuizen.

Mevrouw **Gesthuizen** (SP): Mag ik van u vernemen hoeveel spreektijd ik heb?

De **voorzitter**: U mag zes minuten gebruiken. Ik ben net ook coulant geweest.

Mevrouw **Gesthuizen** (SP): Voorzitter. Wij worden gelukkig goed op de hoogte gehouden van de cyberdreiging. Daar ben ik de Minister zeer erkentelijk voor. Dat wil niet zeggen dat mijn zorgen omtrent de dreigingen die beschreven worden, daarmee zijn weggenomen. Met name het vierde Cyber Security Beeld baart mij toch wel zorgen. Alles wordt eigenlijk alleen maar erger, zo lijkt het. Naast de grote cybercriminelen kunnen nu ook minder ervaren criminelen complexe cyberaanvallen uitvoeren. De dreiging van digitale spionage door statelijke actoren wordt groter. De impact van aanvallen en verstoringen neemt toe. De hoeveelheid malware blijft maar stijgen, net als het aantal slachtoffers van phishingaanvallen et cetera. TNO schatte de schade van cybercriminaliteit in Nederland jaarlijks op minstens 10 miljard euro. Herkent de Minister dat bedrag? Hoe kan dat nu? Hollen we achter de feiten aan? In de voortgangsrapportage is de Minister tamelijk positief over het beleid, maar intussen blijf ik me grote zorgen maken.
Ook de dataverzameling neemt steeds grotere proporties aan, bijvoorbeeld door WholeSecurity. Dit bedrijf stond echter niet alleen, blijkt uit een onderzoek van de Federal Trade Commission naar negen grote Amerikaanse data brokers. Deze bedrijven verzamelen op grote schaal en zonder toestemming persoonlijke data, onder andere om te verkopen. Ik heb ruim zeven pagina's aan soorten data die verzameld worden, uiteenlopend van naam en adres tot kledingvoorkeuren van particulieren, of je graag Elvispoppetjes verzameld en in welke auto je geïnteresseerd bent. Wat doet het NCSC met dit soort informatie? Het gerucht ging overigens ook dat de Nederlandse overheid bij dit soort bedrijven aanklopt om gegevens te kopen. Klopt dat?
Er blijven altijd lekken bestaan waar criminelen en staten misbruik van kunnen maken. Wat dat betreft sluit ik me aan bij de zorgen die al eerder zijn geuit door mijn PvdA-collega. Dat zijn lekken die vaak niet eens per ongeluk bestaan. Ik denk bijvoorbeeld aan de zero days waarmee onze eigen overheid onveiligheid in stand houdt. Ik weet over samenwerking

tussen internetproviders, bedrijven en overheden. Natuurlijk is voorlichting aan eindgebruikers en beheerders ook heel belangrijk. Dat deel ik volledig. Ik lees echter weinig tot niets over de rol van softwarebedrijven als Microsoft, Oracle en Symantec. Zij ontwikkelen elk jaar opnieuw onvoldoende duurzame en slecht beveiligde ICT-producten. Hoe ziet de Minister hun rol in de strijd tegen cybercriminaliteit? Zouden zij ook niet in die samenwerkingsverbanden moeten zitten? Zijn zij straks aanwezig bij de global conference, waar collega's het net al over hadden, die in 2015 in Nederland zal plaatsvinden? Klopt het dat producten van deze softwarebedrijven niet aan de extra veiligheidseisen moeten voldoen die Brussel heeft opgesteld? Wat is daar nu de logica achter? Ze spelen een grote rol bij het voortbestaan van cybercriminaliteit, maar wie doet er nu eigenlijk iets aan? In plaats daarvan worden in mijn ogen de eindgebruikers steeds meer opgezadeld met de extra kosten voor extra beveiliging tegen virussen en malware voor niet-duurzame systemen, inclusief de overheid, met de cybercrimineel als lachende derde. De Minister geeft aan dat de regering inzet op het stimuleren van de ontwikkeling en de aanschaf van veilige hard- en software op de lange termijn. Hoe dan precies en door wie? Hoelang denkt de Minister dat het nog zal duren voordat wij over veiligere – ik snap dat het nooit 100% veilig kan zijn, maar veiliger kan wel – ICT-systemen beschikken?

De buitenlandse veiligheidsdiensten lijken tegen elkaar op te bieden wat betreft investeringen in digitale spionage. Kan de Minister aangeven hoe de samenwerking onderling is? Zitten hier knelpunten? Samenwerking tussen landen is essentieel. Cybercriminaliteit kent immers geen grenzen. Opvallend is de conclusie van het NCSC over spionage door onze bondgenoten. Wie zijn eigenlijk nog onze echte bondgenoten? Hoe zit het met Amerika? Uit documenten die door een journalist van De Correspondent via een WOB-verzoek openbaar werden, blijkt dat Nederland eigenlijk bijna niets doet tegen de Amerikaanse bemoeizucht. Graag krijg ik daarop een reactie.

Gisteren was er nog iets anders in het nieuws, al is dat uiteraard nog niet te verifiëren. Ik vraag me toch af wat het ministerie doet op het moment dat het zo'n bericht krijgt. Ik doel op het nieuws van Snowden. Hij zegt dat de iPhones allemaal voorzien zijn van spyware. Wij hebben dat nog niet ontdekt, maar het zou er wel op zitten. Wat doet de Minister op het moment dat hij dat soort nieuws krijgt? Gaat hij dat verifiëren? Ik zou daar heel graag wat meer inzicht in krijgen. Welke belletjes gaan er allemaal rinkelen op het ministerie?

Ik heb ook nog een paar vragen over botnets. De Minister geeft aan dat er providers zijn die bewust een platform bieden aan botnets en daar dus de benodigde servers voor aanbieden. Welke maatregelen worden er tegen dergelijke providers getroffen? Ik lees daar niets over terug. Kan de Minister voorbeelden noemen van providers die zijn aangepakt? Wanneer worden computereigenaren op de hoogte gebracht als zij het slachtoffer worden van een botnet? Van verschillende kanten heb ik informatie gekregen dat het eigenlijk toch wel makkelijke mogelijk zou moeten zijn om meer te doen ter bestrijding van botnets, onder andere via de request for comments. Ik begrijp echter dat heel veel isp's dat niet, of in ieder geval niet voldoende, uitvoeren. Hoe kan dat? Is de Minister ermee bekend dat deze relatief eenvoudige methoden om botnets tegen te gaan, door de isp's meestal niet worden gebruikt? Is hij bereid om met de isp's in gesprek te gaan en om hen te stimuleren deze methode wel te gebruiken?

Daarnaast meldt een deskundige mij dat botnets actief door inlichtingen- en veiligheidsdiensten kunnen worden ingezet om burgers te monitoren, iets wat de afgelopen dagen in diverse aan Snowden gerelateerde artikelen al in het nieuws was. Hij beweerde dat de AIVD aan de leiband van de NSA loopt. Daar zou ik graag een reactie op krijgen.

Ik heb nog een laatste vraag over het uitgebreide rapport over de scheiding van de netwerken. Dat hele rapport leidt eigenlijk tot de conclusie dat het niet mogelijk is om een eenduidige conclusie te trekken. Ik heb een paar jaar geleden al een heel goed advies gelezen van Bits of Freedom: investeer je tijd en geld vooral in het op de juiste hoogte brengen van de expertise en kennis, onder meer bij de overheid zelf. Is dat niet een veel betere strategie om te kiezen?

Voorzitter: Gesthuizen

De heer **Verhoeven** (D66): Voorzitter. Je hoeft geen internetdeskundige of cyberspecialist te zijn om te zien dat cyber security steeds belangrijker wordt, zoals het Nationaal Cyber Security Centrum benadrukt in zijn vierde beeld. We zijn meer online, we doen meer online, meer apparaten zijn online en diensten zijn steeds vaker online. Dat vergroot de impact van cyberaanvallen misschien wel exponentieel. Ook het belang van de discussie wordt steeds groter en groeit eveneens exponentieel. Dat geeft een legitieme behoefte aan passende maatregelen en passende activiteiten. Tegelijkertijd groeit het bewustzijn van het feit dat zich misbruik kan voordoen onder de vlag van veiligheid. Dat is ook iets waar D66 voor waarschuwt.
Wij hebben een aantal uitgangspunten waarmee we naar cyber security kijken. Het eerste uitgangspunt is dat niet alles wat kan ook wenselijk is. Het tweede uitgangspunt is dat veiligheid en vrijheid heel goed samen kunnen gaan. Je hoeft ze dus niet tegen elkaar uit te ruilen. Het derde is dat cyberhygiëne heel erg belangrijk is en dat je misschien wel 80% van de cybercriminaliteit kunt voorkomen met goede cyberhygiëne. Dat zijn gewoon degelijke, praktische bewustwordingsmaatregelen. Het vierde uitgangspunt is dat je al bij het begin moet nadenken: privacy en security by design. Je moet niet altijd maar beginnen met alles te doen en halverwege eens bekijken waar je uitkomt. Het vijfde is dat samenwerking heel belangrijk is. Lekken en risico's zullen er altijd zijn, maar publiek-private samenwerking kan er heel goed voor zorgen dat je die onder controle houdt.
Ik begin met het Cyber Security Beeld. Ik vind het een heel goed leesbaar, nuttig en waardevol rapport. Laat dat ook eens gezegd zijn. Het laat een aantal heel klare bevindingen zien. Allereerst dat de potentiële impact van cyberaanvallen toeneemt. Ja, dat is logisch, maar het is echt een feit, dus daar moeten we beleid op maken. De Minister doet dat ook en zet een aantal punten in gang. De vraag is wel hoe we nu weten dat de genomen stappen voldoende zijn. Wanneer komt er een evaluatie? Wordt er bijvoorbeeld een weerbaarheidstest toegepast op bepaalde momenten? Is er een meetlat?
Ten tweede is er de bevinding van ICT-duurzaamheid. In dat kader heeft de Minister het over de campagne Alert Online om de cyberhygiëne te vergroten. Ik heb bij mijn familie en vrienden navraag gedaan of zij die campagne kennen, en niemand kende hem. VNO-NCW meldde vorige week op zijn website dat ondernemers ook veel te weinig weten van cybercriminaliteit en cyber security en dat die daardoor misschien wel 30 miljard euro schade hebben. Een andere campagne, namelijk de campagne Geef inbrekers geen kans, is bijvoorbeeld wel heel bekend. Hoe kunnen we de zichtbaarheid van de campagne in overeenstemming brengen met het belang van het onderwerp? Kunnen we er nog een tandje bij zetten? Voorlichting werkt en er zijn goede campagnes, maar dat kan nog wel wat meer.
De derde bevinding is dat er een grote dreiging uitgaat van criminele en statelijke actoren. De Minister noemt de Wet computercriminaliteit III; mijn collega's Tellegen en Van Oosenbrug noemden die wet ook al. Mijn fractie is uitermate kritisch op deze wet. Hij moet echter nog naar de Kamer komen. We hebben er al eerder over gesproken en we hebben onze

zorgen ook al eerder aan de Minister overgebracht. We staan nog steeds open voor discussie. Dit is zo'n punt waarbij veiligheid kan leiden tot verkeerde keuzes, namelijk tot overbevoegdheden. Dat is bij dit ministerie nog weleens een risico, ook gezien de aard van het ministerie.
Twee bevindingen die samenhangen zijn dat de privacy onder druk komt te staan van steeds meer databestandenkoppelingen – mevrouw Gesthuizen had het er ook al over – en dat steeds meer apparaten op internet worden aangesloten: het internet der dingen. Eigenlijk maakt dat zowel de systemen als de datasets, en daarmee de mensen die in die datasets zitten, steeds kwetsbaarder. Hoe groter het systeem, hoe gevaarlijker een lek om in dat systeem te kunnen inbreken, kan zijn. Het zijn dan communicerende vaten. Wat voor schotten worden er zo nu en dan tussen databases gezet? Heeft de Minister een duidelijk beeld van alle verschillende databases die de overheid op alle niveaus heeft en hoe die gekoppeld zijn? Hetzelfde wil ik eigenlijk over het internet der dingen vragen. Sluizen, stoplichten en slimme energiemeters zijn allemaal apparaten die worden aangesloten op het internet. Hoe wordt besloten dat wel of niet te doen? Heeft de Minister daar invloed op? Heeft de Minister daar zicht op? Is het een automatisme waarvan ook weleens wordt gezegd: nee, dat moesten we maar eens even niet doen? Graag krijg ik een reactie op die punten.
In de voortgangsbrief cyber security heeft de Minister het over het stimuleren van innovatie om cyber security te vergroten. Dat kan bijvoorbeeld via de zogenaamde SBIR-programma's. Dat zijn zeer succesvolle programma's voor met name start-ups en mkb in de aanbesteding om innovatie te stimuleren bij kleine bedrijven. Kan de Minister toezeggen – of moeite doen om zover te komen – de SBIR-systematiek ook bij cyber security meer toe te passen?
Tot slot responsible disclosure. We zien dat dit een heel goede manier is om gebruik te maken van de kennis en de betrokkenheid van de ICT-security community. D66 ziet hackers, net als mevrouw Oosenbrug, niet per definitie als criminelen, maar als een waardevolle bron van kennis. Kan de Minister aangeven of de leidraad inmiddels binnen de hele rijksoverheid wordt toegepast? Als dat niet het geval is, waarom niet? Ziet de Minister aanleiding om de leidraad aan te passen naar aanleiding van het vonnis over de hack bij het Groene Hart Ziekenhuis in Gouda?

Voorzitter: Verhoeven

De vergadering wordt geschorst van 14.33 tot 14.44 uur.

Minister **Opstelten**: Voorzitter. Dank voor alle vragen die gesteld zijn. Ik proef daarin een constructieve en hier en daar zorgelijke toon. Ik denk dat we dat delen. Ik mag de Kamer ook danken voor het feit dat een aantal woordvoerders ons Nationaal Cyber Security Centrum een bezoek heeft gebracht. Dat wordt altijd zeer gewaardeerd en werkt ook stimulerend. De gebeurtenissen in de afgelopen maanden laten duidelijk de internationale component van cyber security zien; dat hebben we ook in de documenten opgeschreven. Ze onderstrepen het belang van cyber security en de ambitie van Nederland om uit de strategie langs de lijnen van de inhoud leidend te zijn. Enorm belangrijk is altijd dat er publiek-privaat wordt samengewerkt. Gisteravond had ik de jaarlijkse bijeenkomst met de Cyber Security Raad, waarin de top van het bedrijfsleven in vele geledingen zit. De wetenschap zit er ook in. Professor Bart Jacobs was er. Hij is ook voorzitter van de raad van toezicht van Bits of Freedom. Ik kreeg nog even een klein prijsje van hem. Dat deed hij op zijn eigen wijze. Ik heb daar op mijn eigen wijze op gereageerd door te zeggen dat ik «m nu al voor de derde keer heb gekregen en dat het met de privacy in Nederland dus niet zó erg is gesteld. Dat waardeerde hij zeer. Hij waarschuwde mij nog bij het in ontvangst nemen van de prijs. Er zat een apparaatje in waarmee men

mij vanaf dat moment op de voet zou volgen. Ik heb het vanochtend direct afgeleverd bij mijn eigen deskundigen, dus daar hoeven we ons geen zorgen meer om te maken. Ook de overheid is in die raad stevig aanwezig; ik kom daarop terug.
Ik ga nu niet alles herhalen wat de leden in de cijfers en de beelden hebben gekregen. Ik heb natuurlijk wel veel papieren bij me, maar de leden hebben allerlei vragen gesteld. Ik merkte aan de betogen dat zij alle cijfers tot zich hebben genomen. Dat is belangrijk werk. Ik ga de vragen gewoon langslopen. De woordvoerders zullen zich afvragen wat voor das ik draag. Ik had «m gisteravond ook om. Sommigen zeiden dat ze niet wisten dat ze zouden spelen die avond. Dit is de officiële das van de Global Cyber Space Conference 2015. Die zal op 16 en 17 april in Den Haag plaatsvinden, na Londen, Budapest en Seoul. Ik kom daar graag later nog op terug.
Mevrouw Tellegen heeft gevraagd wie het Nationaal Cyber Security Centrum coördineert. Ik ben coördinerend bewindspersoon voor de cybersecurity. Het centrum voert zijn taken op dit gebied namens mij uit. Het is een onderdeel van de organisatie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid die coördinerend is op het terrein van de cybersecurity en daarmee de spin in het web. Het was voor de heer Schoof gemakkelijk om gisteren bij die bijeenkomst in Hilversum te zijn. Het was voor hem een kort ritje naar de studio van Nieuwsuur waar hij vanaf 22.00 uur te zien was.
Het voortouw voor coördinatie, initiatief en aanpak van cyberproblemen in de vitale sector ligt dus inderdaad bij het Nationaal Cyber Security Centrum. De organisaties blijven zelf verantwoordelijk voor hun cybersecurity. Dat is de kern van het hele verhaal. Er wordt intensief samengewerkt met publieke en private partners waaronder de AIVD en het Ministerie van Defensie. Deze samenwerking verloopt goed. Andere voorbeelden zijn de liaisons bij het Nationaal Centrum en het Nationaal Detectie en Response Netwerk, en de intensieve samenwerking in het kader van de NSS. Als onderdeel van de strategie wordt gesproken over de versterking van de samenwerking bij de analyse van fenomenen als botnets.
Mevrouw Tellegen heeft verder gesproken over de publiek-private samenwerking die in vergelijking met het Verenigd Koninkrijk, in Nederland nog in de kinderschoenen staat. Het Verenigd Koninkrijk certificeert bedrijven en er wordt meer informatie gedeeld. Het is inderdaad stevig bezig met de publiek-private samenwerking. Daarom hebben wij zeer regelmatig op strategisch niveau contact met het Verenigd Koninkrijk. Met de tweede Nationale Cyber Security Strategie hebben wij immers de stap gezet van publiek-private samenwerking naar participatie. Dat is een stapje extra en juist daarin zie ik dagelijks voorbeelden van participatie waarin bijvoorbeeld via de netwerken van het Nationaal Detectie en Response Netwerk intensief wordt samengewerkt. Ik heb daarvan gisteren een paar duidelijke voorbeelden gezien bij het KPN monitoringcentrum waar wij die vergadering hadden. Daar werd ook gezegd dat het bij de aanpak van de problemen belangrijk is dat als een private onderneming zoals KPN informatie krijgt, zij die informatie ook direct kan doorspelen naar de partner die dan nuttig en nodig is. Dat is altijd het Nationaal Cyber Cyber Security Centrum. Wij krijgen ook van die kant de mededeling dat de markt en de buitenwereld de kwaliteit van het centrum prijzen. Ik meen dat dit ook in internationaal opzicht het geval is.
Naar aanleiding van de opmerkingen over het delen van informatie kan ik aangeven dat ik juist om die reden vandaag een wetsvoorstel in consultatie heb gebracht. Het is niet precies zo getimed, maar het komt toevallig goed uit. Het is in ieder geval wel nuttig dat dit nu is gebeurd. Door middel van vertrouwelijkheid zal het delen van informatie worden gestimuleerd. Ik kom daar nog op terug.

Een andere vraag is of het Britse systeem van certificering een optie voor Nederland is. Een actielijn in de Nationale Cyber Security Strategie is het verkennen van de mogelijkheid tot het accrediteren van bedrijven die als digitale brandweer kunnen worden ingeschakeld. Ik weet dat mevrouw Gesthuizen in dit verband graag het woord «brandweer» gebruikt. Je moet daarmee voorzichtig zijn, maar ik meen dat ik het zo wel kan beschrijven. De verkenning vindt dit jaar plaats. Daarin zullen de ervaringen van de Britten worden meegenomen. Een dergelijk systeem past in de lijn van de groeibrief die ik in het najaar van vorig jaar aan de Kamer heb gestuurd over het versterken van de e-commerce. Ik zal de Kamer in de volgende voortgangsrapportage over de strategie nader informeren over deze verkenning.
Vervolgens is nog gevraagd wat de stand van zaken is bij de capaciteitsopbouw en het behalen van de doelstellingen. Het THTC is volledig gevuld, behoudens de gebruikelijke vacatures als gevolg van de uit- en doorstroom. De uitbreiding met 119 fte is gerealiseerd. Wij hebben gisteren complimenten gekregen voor het feit dat de politie de doelstelling van twintig grote zaken naar verwachting heeft gehaald. De politie zal hierover rapporteren in het jaarverslag.
Tijdens de bijeenkomst gisteren kwam naar voren dat bij een combinatie van een actie die in zo'n council plaatsvindt, ook aspecten van werkgelegenheid, arbeidsmarkt en onderwijs aan de orde zijn. Dit geldt natuurlijk niet alleen voor politie, justitie of overheid, maar ook voor het bedrijfsleven. Is het opleidingsniveau op alle fronten voldoende om de goede mensen binnen te krijgen? Cybersecurity is een groeimarkt in Nederland en daarin zijn veel banen te krijgen. Wij moeten natuurlijk de goede mensen krijgen die goed zijn opgeleid. Professor Jacobs van de Universiteit Nijmegen heeft daar gisteren iets over verteld, maar ook de opleidingen op hbo- en mbo-niveau zijn belangrijk en moeten worden verder geholpen. Dit zal ook een belangrijk thema zijn in het werkplan van de Cyber Security Raad.
De vraag is gesteld wat ik zal doen om het bewustzijn van informatiebeveiliging te vergroten. De heer Verhoeven heeft aan zijn kennissen gevraagd naar dit onderwerp, ik heb dat ook gedaan en dan blijkt dat niemand er ooit van heeft gehoord. Er is ook wel eens iemand die positief antwoordt op mijn vraag, maar ik heb de indruk dat dit dan gebeurt om mij een genoegen te doen. Die mensen zijn er nog steeds. Bij het voeren van een campagne mag je geen resultaten op korte termijn verwachten, dat weten wij allemaal. Je moet continu doorgaan. Wij gaan natuurlijk door met Alert Online. Wij zullen alle signalen oppakken om die campagne te verbeteren. Digitale veiligheid begint bij het bewustzijn van de risico's. Consumenten en organisaties kunnen dan maatregelen nemen om die risico's te verkleinen. Daarom ook is het belangrijk dat wij hier voortdurend in investeren. Onze campagne is hiervan een voorbeeld. Ik heb daarover al genoeg gezegd.
Mevrouw Tellegen heeft nog gevraagd naar de uitvoering motie-Hennis. Die vraag was aanleiding voor een interruptiedebatje waarnaar ik met belangstelling heb geluisterd. Het wetsvoorstel brengt het Nationaal Cyber Security Centrum verder in positie. Dat wetsvoorstel is vandaag in consultatie gebracht; het is dus nog niet ingediend. Bij het streven naar het verwerken en delen van informatie met de andere partijen zoeken wij naar een balans tussen vertrouwelijkheid en openbaarheid om die informatie te kunnen delen. Wij hebben al eerder gesproken over het feit dat het heel belangrijk is om bij partners als VNO-NCW draagvlak te krijgen voor het wetsvoorstel opdat men ook gaat melden. Dat is van groot belang voor de nationale veiligheid. Het wetsvoorstel zoals dit nu ter consultatie voorligt, voorziet in het melden van incidenten, vertrouwelijkheid waar dat echt nodig is – dit in lijn met eerdere vragen van de Tweede Kamer – en openbaarheid en het delen van informatie waar dat moet conform de rol van het Nationaal Cyber Security Centrum.

Voorzitter: Gesthuizen

De **voorzitter**: Ik zie dat de heer Verhoeven u een vraag wil stellen

Minister **Opstelten**: Het wetsvoorstel is trouwens nog niet ingediend.

De heer **Verhoeven** (D66): Ik hoor de Minister dit nu weer allemaal zeggen. Toen hij VNO-NCW noemde, ging er bij mij een lampje branden. Ik herinner mij uitspraken van de Minister over de enorme administratieve lasten die bij een te zware meldplicht over de bedrijven zouden worden uitgestort. Hij heeft toen ook grote getallen genoemd. Ik zal ze zo nog even opzoeken voor de tweede termijn, maar ik herinner mij dat bedrijven angstaanjagende bedragen zouden mislopen. Is de Minister van mening dat de meldplicht daarom moet worden afgezwakt?

Minister **Opstelten**: Nee, totaal niet. Het gaat om de effectiviteit van de meldplicht; die is bedoeld voor security breaches. Ik heb de hoofdlijnen nu weergegeven. VNO-NCW heeft die vraag wel gesteld bij een ander wetsvoorstel, maar niet bij dit voorstel. Je moet accepteren dat bepaalde zaken vertrouwelijk kunnen zijn. Daarvoor wordt ruimte geboden in dit wetsvoorstel. Wij zijn tevreden over het resultaat en het draagvlak daarvoor. Het wetsvoorstel is nu in consultatie, dus iedereen komt even terug. Het is ongelooflijk belangrijk dat wij dit nu hebben en dat het straks gaat werken. Dit is een goede uitvoering van de motie-Hennis. Het is knap dat wij dit zover voor elkaar hebben gekregen en nu moeten wij de consultatie afwachten. Ik vraag de Kamer om ons de ruimte te geven om de normale discussie en het debat te voeren. Dit heeft niets met administratieve lasten of dat soort zaken te maken. Er is geen sprake van kosten voor het bedrijfsleven.

De heer **Verhoeven** (D66): Dat is dan een geruststelling. Er zijn inderdaad twee wetsvoorstellen. Ik weet dat dit bij het ene wetsvoorstel misschien een groter issue is dan bij het andere. Als de Minister zich in de consultatie waarin iedereen zich kan melden, niet eenzijdig laat leiden door de belangen van bepaalde grote bedrijven, ben ik voor dit moment enigszins gerustgesteld.

Voorzitter: Verhoeven

Minister **Opstelten**: Door goede ideeën te verzamelen en goede voorbeelden en ervaringen uit te dragen, geeft Nederland gehoor aan de internationale wens om concrete oplossingen te bieden voor uitdagingen in het cyberdomein. Op deze manier ontstaat een bibliotheek van kennis en goede voorbeelden in het cyberdomein op onder meer de volgende punten: responsible disclosure, het bevorderen van awareness, onderwijs, CERT maturity, cybercrime, e-development, privaat-publieke participatie, multistakeholdersamenwerking, en vrijheid in cyberspace. Daarmee krijgt Nederland een internationale platformfunctie voor cyber en krijgt het de beschikking over een rijke verzameling van de beste manieren voor de aanpak van cybersecurity.
Een Nederlandse gezant, oud-minister Rosenthal, reist de wereld rond om ervoor te zorgen dat velen naar de conferentie zullen komen. Dit lukt goed. De Kamer krijgt ook een uitnodiging en ik reken erop dat de leden komen. Het wordt een grote conferentie. Na, Londen, Boedapest en Seoul wordt deze internationale conferentie nu in Nederland gehouden. In Hongarije is het internationale verdrag gesloten.
De slotvraag van mevrouw Tellegen was of de rolverdeling tussen de vier betrokken ministeries bij een crisis duidelijk is. Die rolverdeling is volstrekt helder. Ik ben belast met de coördinatie. Bij een crisis kunnen interventiemogelijkheden worden gebruikt die in de fysieke wereld ook bestaan. Dit

is uiteengezet in de brief van 6 juli 2012. Diginotar was natuurlijk ook een voorbeeld van een crisis. Het Nationaal CrisisCentrum gaat dan aan het werk. Ik zit dat voor tenzij het in de gegeven situatie absoluut noodzakelijk is dat de Minister-President dat doet zoals dat het geval was bij de MH17-crisis. Ik heb dat gedaan bij Diginotar. Destijds was Minister Donner de eerstverantwoordelijke, omdat het de rijksoverheid betrof en hij als Minister van Binnenlandse Zaken naar voren moest treden. Na alle evaluaties en onderzoeken kan ik nu toch wel zeggen dat wij dat toen goed hebben aangepakt.
Ik voeg hier nog iets aan toe. Gisteren kwam tijdens de council naar voren dat wij met onze incidenten – dat zijn toch vaak wake-upcalls voor de organisatie – veel meer en soms duidelijker naar buiten moeten komen. Wij moeten scherper aangeven wie wat moet doen. Ik heb die interventie van harte onderstreept, maar de verantwoordelijkheden zijn volstrekt helder.

Mevrouw **Gesthuizen** (SP): Even een verhelderende vraag. De Minister zegt dat hij in principe de zaken voorzit in geval van een crisis, tenzij de Minister-President de aangewezen voorzitter is. Dat is heel duidelijk. Hij refereerde aan het feit dat toenmalig Minister Donner van Binnenlandse Zaken de kar trok. Zou dat nu nog steeds zo gaan?, Immers, sinds Diginotar is er natuurlijk wel het nodige veranderd. Is het dan niet de Minister van Veiligheid en Justitie die als eerste opereert, gezien de overkoepelende verantwoordelijkheden?

Minister **Opstelten**: Het is afhankelijk van de situatie. Het sloeg neer op de departementen. Nogmaals, iedereen is in de eerste plaats verantwoordelijk voor zijn eigen onderdeel. Ik zal het niet van iedereen overnemen. Wij hebben ook een dergelijke situatie gehad bij banken. Toen was ik in het weekend belast met de coördinatie en de operatie. Op maandag was er een grote bijeenkomst met de vier CEO's van de banken, want de banken moesten het zelf oplossen. Ik treed niet in de verantwoordelijkheden van mijn collega's om alles op te lossen, maar ik zorg er wel voor dat degenen die verantwoordelijk zijn binnen het crisismanagement, doen wat zij moeten doen.

Mevrouw **Gesthuizen** (SP): Ik vind dat heel verstandig van de Minister. Ik zou ook zeker niet alle problemen van mijn collega's willen oplossen. Zij moeten dat in de eerste plaats zelf doen.

Minister **Opstelten**: Dat is wel jammer.

Mevrouw **Gesthuizen** (SP): Absoluut. Ik vind dat ook wel eens jammer. Ik heb dit echter gevraagd, omdat ik van mening ben dat er sinds Diginotar wel iets is veranderd. In mijn ogen heeft de Minister van Veiligheid en Justitie sindsdien een veel duidelijker, coördinerende spin-in-het-web-rol. Als er sprake is van een crisis zoals bij Diginotar, dan kun je natuurlijk ook altijd naar de Minister van BZK kijken als het om de nationale veiligheid gaat. Als er echter sprake is van een veiligheidssituatie, dan is het naar mijn mening belangrijk dat de Minister van Veiligheid en Justitie in beeld is.

Minister **Opstelten**: Dan is dat precies aan de orde, maar wij spraken nu over de voortgang. Kan de Belastingdienst werken, kan het OM werken, werkt DigiD? Die vragen waren toen aan de orde. Minister Donner en ik hebben ook samen het Kamerdebat gevoerd. Ik heb mij daar niet aan onttrokken en ik zal dat ook in de toekomst zeker niet doen. Als de nationale veiligheid in het geding is, ben ik verantwoordelijk. Ik ben de spin in het web. Wij brengen de partijen bij elkaar en laten iedereen doen wat hij of zij moet doen.

Mevrouw **Tellegen** (VVD): De Minister refereerde aan de uitkomst van een bijeenkomst van gisteravond over de wake upcalls en de incidenten waarvan wij meer moeten leren. Heb ik goed begrepen dat hij van mening is dat het zaak is dat wij terugkijken om te zien wie welke verantwoordelijkheid heeft genomen? Wat bedoelde hij precies?

Minister **Opstelten**: Wat ik zei: een incident is helaas vaak een wakeupcall waaruit blijkt hoe je dingen moet aanpakken. Diginotar is daarvan een goed voorbeeld. Daarvoor werd er toch betrekkelijk relativerend gesproken over cybersecurity – ik heb dat niet gedaan – maar daarna gingen ieders ogen open. Als er vragen worden gesteld na een incident, kun je de hoofdspelers meer naar buiten laten komen en kun je vertellen wat zich heeft afgespeeld, hoe het is aangepakt, wat er beter had gekund en welke maatregel moet worden genomen.
Ik kom bij de vragen van mevrouw Oosenbrug. Zij heeft gevraagd of internet een omgeving is geworden van opsporing en massasurveillance. Ik herken dit beeld, vertrouwen in het internet is een belangrijk punt. Juist met de acties van de strategie voorzien wij in de balans tussen vrijheid, veiligheid en maatschappelijke groei.
Haar volgende vraag was wat de Herijking Vitaal inhoudt en hoe de stand van zaken is. In lijn met de toezegging die ik aan het einde van 2013 aan de Kamer heb gedaan, voert het kabinet een herijking uit van de vitale infrastructuur, processen, diensten en locaties. De interdepartementale herijking leidt tot een herdefiniëring van de vitale infrastructuur in Nederland, inzicht in de belangrijke kwetsbaarheden van deze infrastructuur en, indien nodig, all-hazardsafspraken om de weerbaarheid te verhogen. De herijking wordt in afstemming en samenwerking met alle relevante partners opgepakt, van ministeries en private vitale organisaties tot aan de veiligheidsregio's. Het ligt in de planning de Kamer medio dit jaar over de resultaten van de herijking te informeren in de brief over de nationale veiligheid.
Mevrouw Oosenbrug heeft gevraagd of SURFnet is meegenomen in de verkenning naar gescheiden netwerken. Ik ben blij dat zij zich herkent in de conclusie van de verkenning dat een volledig gescheiden netwerk geen haalbare en wenselijke optie is. Wij hebben dit extern laten toetsen. De oplossing van de experts van SURFnet is wel degelijk meegenomen in de verkenning. De ontwikkeling van onbelichte glasvezelkabels is juist een van de businesscases die wij in toenemende mate gebruikt zien worden. Risicoafweging speelt daarbij uiteraard een rol. Dit is een van de onderwerpen die wij met de vitale sectoren bespreken. Minister Blok van Wonen en Rijksdienst neemt dit ook mee bij beslissingen over de doorontwikkeling van overheidsnetwerken. Ik kan aanvullend nog melden dat wij zeer nauw samenwerken met SURFnet bijvoorbeeld in het Nationaal Detectie en Response Netwerk.
Dan is nog gevraagd hoe wij aankijken tegen het delen van apparatuur en NaWas. Ik juich de initiatieven zoals de Nationale Wasstraat toe. In dit kader delen providers apparatuur die louter voor henzelf niet rendabel is. Ik heb in de brief over de verkenning gescheiden netwerken reeds geschreven dat ik hierbij een stimulerende en faciliterende rol voor de overheid zie. Zo is het Nationaal Cyber Security Centrum betrokken bij de ontwikkeling van een diversiteit aan innovatieve oplossingen bijvoorbeeld door constructief mee te denken. Daarnaast stimuleren wij uiteraard onderzoek naar innovaties door middel van het SBIR-instrument.
In antwoord op de vraag hoe de isp's een actieve rol op zich hebben genomen, kan ik melden dat op zeer constructieve wijze wordt samengewerkt met de isp's. Zij hebben zich verenigd in het initiatief AbuseHUB waarin informatie wordt gedeeld over botnet-besmettingen van klanten. Ik ben van mening dat internetserviceproviders de handschoen actief hebben opgepakt bij de aanpak van botnets.

Mevrouw Oosenbrug sprak verder over de hackers en de responsible disclosure. Het is goed om hier wederom over te spreken. Ik heb eerder al gezegd dat hacken als zodanig strafbaar is. Dat is het uitgangspunt. Als er beleid voor responsible disclosure is, is er sowieso geen reden voor zorgen over de hackers. Recente uitspraken laten zien dat ook de rechter deze ruimte biedt. Ik wijs erop dat Nederland het enige land ter wereld is waar de overheid zo'n officieel standpunt heeft ingenomen. Wij zullen daar tijdens de conferentie in april heel nadrukkelijk uiting aan geven.
De functionaliteiten van het landelijk meldpunt internet-oplichting blijven in de nieuwe organisatie van de Nationale Politie gehandhaafd. Ik weet niet exact op welke wijze. Zelfs als Minister moet je bescheiden zijn in je bemoeizucht met de korpsleiding. Als een en ander in balans blijft, wordt dat ook aan die kant gewaardeerd.
De Vereniging AbuseHUB is zelf verantwoordelijk voor de informatiebeveiliging. Hierbij geldt dat bij de verwerking van persoonsgegevens de Wpb van toepassing is. In het kader van de deelnemende bedrijven kan in aanvulling hierop de Telecommunicatiewet van de Minister van Economische Zaken van toepassing zijn.

De **voorzitter**: Ik wijs erop dat Wbp staat voor de Wet bescherming persoonsgegevens.

Minister **Opstelten**: Dat weet toch iedereen, maar niettemin dank voor de aanvulling.
Mevrouw Gesthuizen heeft gevraagd of ik mij herken in het bedrag van 10 miljard dat door TNO wordt genoemd. Ik kan dit getal niet bevestigen. TNO is TNO. In veel onderzoeken worden grote bedragen genoemd, maar die zijn zeer lastig vast te stellen. Ik ben daarom voorzichtig om nu een bedrag te noemen. Ik maak mij wel zorgen over de problematiek. In sommige onderzoeken komt Nederland sterk naar voren. Wij hebben een goede digitale infrastructuur in ons land en er wordt veel tegen cybercrime gedaan. In veel andere landen is meer onbekend. Je ondervindt er soms nadelen van als je heel actief bent, in een breed gezelschap de diepte induikt en niet geheimzinnig met de gegevens omgaat.
Zij heeft gevraagd hoe de samenwerking tussen de spionagediensten verloopt en wie onze bondgenoten zijn. Wij werken met iedereen samen die wil werken aan een veilig internet. Wij zien dit terug in onze multidisciplinaire en multistakeholderaanpak van de Global Conference on Cyberspace. Dat is daarvan een duidelijk voorbeeld.
Een andere vraag van mevrouw Gesthuizen was wat het Nationaal Centrum met de informatie van de data brokers doet. Mijn antwoord op haar vraag of het klopt dat Nederland ook data koopt, is nee. Ik meen dat ik dit al eerder heb gezegd. Ik zie het nog voor me dat ik ook toen met «nee» antwoordde. Het is bijvoorbeeld ook niet gebeurd in de casus van de hold security waarover ik de Kamer eerder schriftelijk heb geïnformeerd.
Zij wijst erop dat er een beeld wordt geschetst van toenemende criminaliteit en spionage in Nederland en zij vraagt of ik de zaak nog wel onder controle heb. Ik vind «onder controle» een moeilijk begrip, want dat zou ook kunnen betekenen dat het niet gebeurt. Wij moeten maximaal doen wat noodzakelijk is, maar dit is ook verder in ontwikkeling. De overheid en het bedrijfsleven zetten gezamenlijk de benodigde stappen. Beide onderkennen de scherpte van de problematiek. Die wordt niet gebagatelliseerd en er wordt niets gesust. Het is en blijft echter van belang om voortdurend bij te blijven bij de ontwikkelingen. Dit vergt de inzet die wij onder andere met de cyberstrategie beogen.
Het kabinet zet in op de stimulering van de ontwikkeling van veilige harden software door de toepassing van standaarden. In 2014 is een overzicht gemaakt van relevante standaarden waarbij onderscheid is gemaakt naar doelgroep en de mate van toepassing. Die standaarden kunnen worden

gebruikt voor het vergroten van de digitale veiligheid van vitale processen. Er is een publiek-privaat platform voor internetstandaarden ingericht dat deze problematiek verder oppakt.
Over de vraag of wij de leidraad responsible disclosure moeten aanpassen naar aanleiding van de uitspraak van de rechter heb ik al iets gezegd. Die uitspraak sluit aan bij mijn inspanningen inzake responsible disclosure.
In gevallen waar een responsible disclosurebeleid bij een organisatie bestond, is geen aangifte gedaan en/of vervolging ingesteld. Daarmee geeft het responsible disclosurebeleid een stevig handvat voor wat wel en wat niet kan. Daarmee zijn er dan ook geen redenen om een leidraad aan te passen. Wel is er de inzet om die actief aan de man te brengen.
Is de leidraad binnen de hele rijksoverheid al actief, zo vroeg mevrouw Gesthuizen. Ja. Over het punt van de gescheiden netwerken denk ik nu van mijn kant hardop na. Is het niet veel beter om de kennis op orde te brengen, zoals Bits of Freedom bepleit? Dat heb ik gisteren ook gehoord en dat toen onderschreven. Dat is natuurlijk niet het enige. Ik ben altijd erkentelijk voor de bijdrage van Bits of Freedom. Ik mag de mensen daarvan zeer, zonder dat zij te hoeven zeggen dat dat geheel wederzijds is. Ik luister wel naar ze, ook bij de voorbereiding van wetsontwerpen. Het is goed om op het scherp van de snede soms van mening te verschillen. Wij zullen zeker nog kijken naar dit rapport. In het algemeen is kennis altijd noodzakelijk om digitaal veiliger te worden, dus inzetten op kennis is altijd goed en dat stopt niet.
Wat vind ik van de uitspraken van de heer Snowden in Nieuwsuur? Ik was van plan om naar de heer Schoof te kijken, dus ik kwam ook de heer Snowden tegen, want die ging daaraan vooraf in de Volkskrant van die ochtend. Uit niets van wat ik vanuit mijn positie zie, kan ik afleiden dat de Nederlandse diensten aan de leiband van de Amerikanen lopen, integendeel. Ik ervaar de diensten vanuit mijn verantwoordelijkheid als uiterst professioneel en autonoom in hun werkzaamheden. Zij worden natuurlijk in het systeem ook goed in de gaten gehouden door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten onder leiding van de heer Brouwer. Ik hoef mevrouw Gesthuizen daarover niets te zeggen. Daarbij is sprake van goede waakzaamheid jegens de Kamer.
Zullen softwarebedrijven zoals Microsoft en Symantec ook aanwezig zijn bij de global conference? Geen enkele partij heeft volledige controle over zeggenschap in cyberspace. De vele partijen en factoren zijn in toenemende mate met elkaar verbonden en van elkaar afhankelijk in een complexe omgeving waarin continu naar een balans moet worden gezocht tussen vrijheid, veiligheid en maatschappelijke en economische groei. Daarom is het noodzakelijk dat alle stakeholders actief participeren op basis van een heldere rolverdeling en een grote mate van transparantie. Voor het welslagen van de global conference is het dan ook essentieel dat alle relevante partijen deelnemen aan de conferentie. De global conference is een multistakeholderbijeenkomst. We gaan uit van 1.300 genodigden, waaronder de leden van uw Kamer, deelnemers van aangeschreven overheden, internationale organisaties, bedrijven, de technische internetgemeenschap, academici en burgerbelangengroepen, waaronder de genoemde softwarebedrijven.
Wat doet de Minister eigenlijk als er weer een Snowden- onthulling komt? Conform de reguliere rol van het Nationaal Cyber Security Operations Center kijken wij naar de impact voor de nationale overheid en de vitale sectoren. Niets ontgaat ons daarbij.
Ben ik bekend met de methode request for comments? Ga ik providers hierop aanspreken? Ja, daar ben ik mee bekend. Dit gaat om het gebruik maken van de best practices in de aanpak van malware en dergelijke toepassingen die een impact kunnen hebben op de bedrijfsvoering. Ik zal dit met mijn collega van Economische Zaken meenemen in ons gesprek met de internetproviders.

Mevrouw Gesthuizen vroeg of de internetproviders meedoen met de aanpak van de botnets. Die aanpak is gericht op het criminele netwerk achter het botnet, met successen. Meestal is er sprake van een goede samenwerking met de providers. Inmiddels is een pilot gestart om de omvang van de bad hosting beter in kaart te brengen en om tot een gezamenlijke aanpak te komen. Veel providers zijn zich er niet van bewust dat ze criminelen faciliteren. In dat opzicht is de aanpak dus zeer nadrukkelijk effectief om hiervoor aandacht te vragen.
De heer Verhoeven dank ik voor zijn heldere uitgangspunten. Ik ben zo vrij om te zeggen dat ik die gewoon kan overnemen.

Mevrouw **Gesthuizen** (SP): Het is toch een wat ingewikkeld punt over de isp's en de botnets. De rest van mijn vragen bewaar ik uiteraard voor de tweede termijn. De Minister heeft al een paar keer in zijn beantwoording aangegeven dat het best goed gaat, dat men met elkaar in overleg is, dat de isp's daaraan meedoen en dat hij nog een nader gesprek met hen aangaat. Van de beproefde methoden die nu al mogelijk zijn kan ik me voorstellen dat ze niet echt vrij zijn van enig nadeel, want je moet natuurlijk ook uitkijken dat je de netneutraliteit niet al te zeer schendt. Kan de Minister mij nu vertellen of de methoden die er zijn om botnets tegen te gaan, bijvoorbeeld het filteren van vaste IP-adressen en het blokkeren van geïnfecteerde systemen, op dit moment al behoren tot het goed gebruik? Zo ja, geldt dit dan alleen voor heel grote isp's of voor het overgrote merendeel van de isp's? Dat is namelijk niet de informatie die mij ter ore is gekomen.

Minister **Opstelten**: Mag ik dit even voor de tweede termijn bewaren om er dan specifiek op te reageren?

De **voorzitter**: Waarbij de vraag helder is overgekomen, dus die hoeft niet meer herhaald te worden. Het antwoord komt in tweede termijn.

Minister **Opstelten**: Het antwoord komt in tweede termijn. Is dat goed?

De **voorzitter**: Bij dezen.

Minister **Opstelten**: Dan kom ik bij de heer Verhoeven, die zei dat de privacy onder druk komt te staan van de dataverzameling en het internet en die vroeg wat voor schotten daartussen worden gezet. Het risico van verlies van privacy komt ook in het Cyber Security Beeld Nederland naar voren. In de strategie is dat scherp aangegeven. Privacy by design door het vormen van schotten kan noodzakelijk zijn. Laten wij daar tijdens het AO Dataretentie en privacy op 26 maart verder over spreken. Ik vind natuurlijk dat de balans er altijd moet zijn, maar het beleid moet ook effectief zijn.
De heer Verhoeven heeft gevraagd of ik kan toezeggen de SBIR systematisch toe te passen. Ja, sterker nog, die passen wij inmiddels al toe. Sinds 2012 zijn er twee rondes in dit kader geweest. Medio dit jaar kan ik de Kamer definitief zeggen dat er een derde ronde komt. De gesprekken daarover zijn op dit moment gaande.
Vindt een evaluatie plaats van de maatregelen? Ik ben het met heer Verhoeven eens dat evaluatiemonitoring belangrijke onderdelen van de reguliere beleidscyclus zijn. Daarom evalueren wij de volgende drie sporen. Ten eerste via de reguliere bedrijfsdoorlichting van de begroting, die ten aanzien van cyber security voor volgend jaar is voorzien. Ten tweede heb ik de Inspectie Veiligheid en Justitie gevraagd om de effecten van de adviezen van het NSCS te evalueren. Ten derde wijs ik erop dat wanneer de Wet meldplicht en gegevensverwerking cyber security in werking is getreden, wij die na twee jaar zullen evalueren.

Heb ik invloed op de mate waarin apparaten steeds meer aan internet worden gekoppeld? Het internet der dingen is relevant. ICT zit ook steeds prominenter in de portefeuille van mijn collega's. Ik adviseer vanuit mijn coördinerende rol hoe hiermee om te gaan. Het is belangrijk om daar waar nodig normen en standaarden op te stellen. Daartoe is door mijn collega van Economische Zaken het Platform Internetstandaarden ingericht.
De uitgangspunten die de heer Verhoeven in zijn betoog heeft aangegeven, zijn ook een leidraad in ons denken.

De **voorzitter**: Is er van de zijde van de Kamer behoefte aan een tweede termijn? Die is er, want mevrouw Gesthuizen heeft nog een vraag openstaan en ook de andere leden willen nog heel kort een inbreng leveren. We hebben daar nog alle tijd voor. De spreektijd is maximaal twee minuten per fractie.

Mevrouw **Tellegen** (VVD): Voorzitter. Ik dank de Minister voor zijn beantwoording. In mijn eerste termijn heb ik gevraagd om een integrale aanpak. De Minister heeft naar mijn mening een mooi beeld geschetst van hoe dat nu werkt.
Ik ben vooral heel blij met datgene wat de Minister heeft gezegd over het voorbeeld dat het Verenigd Koninkrijk heeft gegeven. Dan gaat het om het systeem van certificering. Bij ons staat dat weliswaar nog in de kinderschoenen, maar dit is wel de kant die we op moeten bewegen. Dat vindt de VVD van belang. Ik ben blij met de toezegging, al is dat misschien een groot woord, van de Minister dat er intensief contact met het Verenigd Koninkrijk bestaat en dat de Kamer erover wordt geïnformeerd hoe dit verder wordt opgepakt. Bij de certificering is het van belang dat we met een lijst werken van bedrijven die het vertrouwen van de overheid krijgen om daarmee in toenemende mate samen te werken. Wij zien de reactie met interesse tegemoet, met de verdere informatie over het systeem dat de Britten al veel verder hebben ontwikkeld.
Wat ik verder interessant vind, zijn de opmerkingen van de Minister naar aanleiding van mijn vraag over de rol van de politie en het THTC-team, het opleidingsniveau en de markt die er ligt. Er liggen een heleboel banen in het verschiet. Net als ICT is ook cyber security een terrein waarop Nederland een voortrekkersrol kan spelen. Dat is een positieve ontwikkeling. Mooi dat dat ook in het werkplan van de Cyber Security Raad wordt meegenomen.
Verder heb ik de Minister horen zeggen dat de campagne Alert Online weliswaar niet al te veel navolging krijgt op dit moment maar dat het des te belangrijker is dat die wordt voortgezet en dat wordt bekeken hoe die nog intensiever over het voetlicht kan worden gebracht, ook voor ondernemers.
Over de uitvoering van de motie-Hennis is het nodige gezegd. Wij zien dat wetsvoorstel na de consultatie met belangstelling tegemoet.

Mevrouw **Oosenbrug** (PvdA): Voorzitter. Allereerst natuurlijk dank aan de Minister voor de uitgebreide beantwoording.
Ik ben heel blij dat ook deze Minister de hackers warm omarmt, omdat het toch over sociaal-maatschappelijk betrokken mensen gaat. Ik zou wel graag willen dat in de volgende brief die over responsible disclosure zal verschijnen niet meer wordt gesproken van goedwillende melders of hackers, omdat dat in mijn ogen toch vaak dezelfde mensen zijn.
Over het Meldpunt Internetoplichting kreeg ik een heel mooi en warm antwoord van de Minister, maar ik vind dat niet concreet genoeg, dus ik ga toch proberen een wat concreter antwoord te krijgen omdat juist dit iets is wat ertoe bijdraagt om het internet veiliger en toegankelijker te maken. De signalen die ik krijg, zijn dat dit meldpunt niet per 1 maart aanstaande van start kan gaan. Dat zou ik heel jammer vinden omdat juist

dit een bewezen succesvol meldpunt is waar heel goede resultaten uitrollen. Ik begrijp dat de Minister niet de politie kan opdragen dingen te doen, maar ik wil toch een iets concreter antwoord om te zorgen dat dit belangrijke meldpunt doorgang kan vinden, ook om internetoplichting te blijven aanpakken en het vertrouwen in het internet te herstellen.

Mevrouw **Gesthuizen** (SP): Voorzitter. Dank aan de Minister voor de beantwoording.
Ik heb mijn vraag net al duidelijk gesteld over de isp's en de aanpak van botnets.
Verder zegt de Minister dat met de isp's zeer constructief wordt samengewerkt. Het is goed om dat te horen maar ik vraag me wel af of dat voor alle isp's geldt. Zo niet, dan wil ik graag weten of de Minister hier kan zeggen voor welke isp's dat niet geldt en welke maatregelen zouden kunnen worden genomen tegen onwelwillende isp's.
Op zich is het prettig dat de Minister zegt dat hij de 10 miljard schade van TNO niet herkent. Ik zag dat de NRC-check ook een onvoldoende opleverde, doordat de NRC het ook te kort door de bocht vond om er zomaar 10 miljard euro op te plakken. Om welke bedragen gaat het dan wel? Is het niet verstandig om daarin een beetje te investeren zodat wij wel een schatting kunnen geven van wat de schade is?
Ik had nog een specifieke vraag gesteld over de Brusselse veiligheidseisen, namelijk of ze nu wel of niet gelden voor de softwarebedrijven. Daarop heb ik geen antwoord gekregen. Dat zou ik alsnog graag ontvangen

Voorzitter: Gesthuizen

De heer **Verhoeven** (D66): Voorzitter. Het is natuurlijk mooi dat de Minister de uitgangspunten van D66 zegt te omarmen waar het gaat om de benadering van deze materie. Als de Minister dat zegt, zal hij dat ook zeker doen. Zo nu en dan twijfelen wij daar wel eens aan, maar op sommige momenten ook niet.
Ik heb nog een ander uitgangspunt niet genoemd, waarvan ik de Minister vraag of hij dat ook omarmt, namelijk dat je niet al te direct moet overgaan tot het uitbreiden van bevoegdheden om cyberproblemen op te lossen maar dat je ook binnen de bestaande mogelijkheden moet kijken naar het oplossen of wegnemen van dreigingen. Volgens mij is de uitbreiding van bevoegdheden een reflex die ook bij het ministerie wel eens bovenop de plank ligt. Desalniettemin dank ik de Minister.
Ik kom bij de campagne, in dit geval niet die voor 18 maart maar de campagne om ons allemaal Alert Online te krijgen. Gaat de Minister naast zijn toezeggingen om daar meer aan te gaan doen en het wat verder verspreid te krijgen in de hoofden van mensen ook daadwerkelijk de intensiteit vergroten? Gaat hij andere kanalen inzetten? Gaat hij nieuwe manieren bedenken? Waar zit concreet de verbreding of de intensivering van die campagne? Dat vind ik belangrijk om te weten.
Tot slot ben ik niet tevreden met de antwoorden van de Minister over het koppelen van alle bestanden, waarvan hij zei dat we dat op 26 maart bij het AO Dataretentie en privacy misschien beter kunnen behandelen. Daarin wil ik wel meegaan, maar ik vraag de Minister om daar dan ook iets over te schrijven of te zeggen, voorafgaand aan dat algemeen overleg. Anders stel ik over twee maanden dezelfde vraag en word ik weer met een kluitje in het riet gestuurd. Ik zou nu wel eens van de Minister willen weten wat hij op dit moment weet. Heeft hij een overzicht van bestanden die bij verschillende gemeenten, uitvoeringsinstanties et cetera allemaal aan elkaar gekoppeld worden? In het beeld van het NCSC staat gewoon dat dit een toenemend fenomeen is. Ik heb van de Minister niets gehoord om concreet te krijgen waar, hoe en waarom het meer wordt, of wie zegt: doe het nu eens niet. Als we daarop geen grip hebben, kunnen

we er op 16 maart ook niet waardig over praten. Is de Minister bereid om iets van zijn beeld van al die bestanden met ons te delen? Als hij dat niet wil, is dat ook informatie die ik graag hoor.
Tot slot een vergelijkbare vraag over het aansluiten van al die apparaten. Ook dat is iets wat ik als sluipmoordenaar beschouw en wat in het beeld van het NCSC naar voren komt. Dit gebeurt steeds vaker. Op allerlei bestuurslagen wordt gewoon besloten om wel een sluis, een stoplicht, een apparaat, een slimme meter, een bestand hier of een database daar te koppelen aan het internet omdat dat kan. Dat lijkt zo mooi. Het eerste uitgangspunt van D66: het kan, dus laten we het dan ook maar doen; het lijkt wel leuk en handig. Maar er wordt vaak niet over nagedacht wat de gevaren zijn. Heeft de Minister grip op die sluipmoordenaar? Hij doet er nu het zwijgen toe. Ik vind dat hij die sluipmoordenaar nauwlettend in de gaten moet houden omdat zijn eigen NCSC er in het Cyber Security Beeld nadrukkelijk op wijst. We krijgen dat stuk, wij lezen het en maken ons er zorgen over. Dan kan de Minister niet zeggen: we houden het in de gaten, reken op mij. Graag iets meer concreetheid op dat punt. Dat zou ik waarderen.

Voorzitter: Verhoeven

De vergadering wordt geschorst van 15.40 tot 15.43 uur.

De **voorzitter**: Dan gaan we verder met de laatste akte van dit algemeen overleg, namelijk de beantwoording in tweede termijn van de zijde van het kabinet. Ik geef het woord aan de Minister van Veiligheid en Justitie.

Minister **Opstelten**: Voorzitter. Ik dank mevrouw Tellegen voor haar bijdrage in tweede termijn over het certificeren en de voortgang daarvan en over de ontwikkeling in het Verenigd Koninkrijk. De resultaten daarvan zullen wij, net als andere informatie, opnemen in de voortgangsbrief die aan het einde van dit jaar zal verschijnen. Daarvoor is de conferentie natuurlijk ook van belang.
Mevrouw Oosenbrug zeg ik nog een keer dat ik niets terugneem van wat ik heb gezegd over de responsible disclosure. Ik zal bij een volgende brief daarover de kwalificatie rond de hackers heel voorzichtig en goed weergeven. Zij merkt dat ik met een zekere trots over dat onderdeel spreek. We hebben echt vernieuwend werk gedaan, ook na een goede discussie in deze Kamer.
Dan het Landelijk Meldpunt Internetoplichting. Ik wil hier wel even scherp naar kijken. Het streven is erop gericht om de functie ononderbroken voort te zetten, maar een garantie kan ik nu nog niet geven omdat ik de informatie nog niet heb. Ik kom zo dadelijk ook nog met een verzoek om de Kamer schriftelijk te beantwoorden naar aanleiding van een vraag van mevrouw Gesthuizen in een brief, zodat ik wat specifieker en beter kan doorvragen bij de korpsleiding dan wanneer ik deze vraag hier op afstand zou beantwoorden.

Mevrouw **Tellegen** (VVD): Ik hoor een kans om dan misschien ook in dezelfde brief de afstemming met het Verenigd Koninkrijk over de certificering mee te nemen, want de voortgangsrapportage kon pas aan het eind van het jaar. Dat lijkt mij laat als we ergens in maart al een conferentie houden.

Minister **Opstelten**: Nee, die is niet in maart maar in april. De brief, die ik hierbij toezeg, heb ik in gedachten over twee weken. Geef ons nu ook de kans om wat tot stand te brengen. Ik heb de Kamer geïnformeerd over de stand van zaken. Wij moeten nog een boel doen. Dan hebt u ook veel meer aan die brief en kunt u daarna zeggen dat het allemaal gerealiseerd is dankzij u, toen u deze vraag stelde.

De **voorzitter**: De Minister zegt eigenlijk dat geduld een schone zaak is. Mevrouw Tellegen knikt dat dat in dit geval terecht is. De Minister gaat verder met zijn beantwoording.

Minister **Opstelten**: Dan kom ik bij mevrouw Gesthuizen en haar achtergebleven vraag, of alle mogelijkheden om botnets aan te pakken goed genoeg worden benut door de isp's. Ja, op alle vlakken is er voldoende actie. Dat hebben wij net even vastgesteld. Zo heeft mijn collega van Economische Zaken het eerder genoemde Platform Internetstandaarden ingericht. Daarbij komen ook veiligheidsstandaarden tegen botnets aan de orde.
Dan de volgende vraag van mevrouw botnet, eh mevrouw Gesthuizen.

Mevrouw **Gesthuizen** (SP): Als de Minister mij zo ziet ...

Minister **Opstelten**: Dat is een compliment, want ik ben er helemaal vol van en ik ben erop gekleed! Wat nu als isp's niet meedoen? Dan is er een strafrechtelijke aanpak. Die is vaak heel lastig, maar er wordt soms wel naar gekeken. Als wij het echt niet kunnen accepteren, dan zetten wij ook door.
Over de schade van 10 miljard heb ik het voldoende gehad, maar daarover kunnen wij misschien ook in het volgende Cyber Security Beeld wat meer zeggen. Ik blijf daar altijd voorzichtig in, want wij zijn per slot van rekening wel de overheid.
Over de Brusselse veiligheidseisen wil ik de Kamer schriftelijk informeren omdat ik er anders een te algemeen antwoord over zou geven.
Ik ben het helemaal eens met de heer Verhoeven dat wij niet in de overheidsreflex moeten schieten van nieuwe wetten als er iets is gebeurd. Dus laten wij eerst kijken of we met het bestaande instrumentarium uit de voeten kunnen om een probleem op te lossen en dan pas bekijken of wij iets extra's moeten doen.
De volgende campagne Alert Online zal zich intensiever en directer moeten richten tot de burgers en het mkb, niet alleen tot onze vrienden, want die weten het inmiddels. Ik vraag altijd aan de mensen die het doen om slimme, eigentijdse campagnemiddelen te verzinnen en geen traditionele als die niet werken.
Wat het koppelen van alle bestanden betreft, ben ik bereid te bekijken of ik daarvan een overzicht kan bieden. De heer Verhoeven zei dat hij het ook wil horen als ik dat niet kan. Ik zal een oprechte poging doen, zonder daarin te overdrijven, voor het AO van 26 maart.
Heb ik grip op de sluipmoordenaars? Niemand kan daar volledig grip op hebben. Als ik ja zou antwoorden op deze vraag, zou ik niet deugen. Wel subsidiëren wij innovatieve projecten om hier beter grip op te krijgen. Dit vindt natuurlijk ook binnen de overheden op alle niveaus plaats. Wij gaan niet over alle niveaus.

Voorzitter: Gesthuizen

De heer **Verhoeven** (D66): Wie kan op de rem trappen op het moment dat een gemeente, een waterschap, een ministerie of een uitvoeringsinstantie zegt: we gaan nu dit apparaat of deze groep servers op een bepaalde manier aan het internet koppelen omdat dat kan, dus dan zal het wel iets opleveren? Is dat iemand bij het NCSC of iemand op het ministerie? Wie kan dan zeggen: laten we dit wel of niet doen?

Voorzitter: Verhoeven

Minister **Opstelten**: Wij hebben de kennis, die natuurlijk ook naar ons toe moet komen, en het overzicht. Wij adviseren de betrokken bewindspersoon – dat kan bijvoorbeeld BZK zijn als het om gemeenten gaat – om

zich direct tot de gemeenten te wenden. Of bij de waterschappen kan het I en M zijn, die wij dan adviseren om zich tot de waterschappen te wenden. Wij zijn de spin in het web, maar wij grijpen niet direct in. Wij rukken niet zoals de brandweer met gillende en loeiende sirenes uit maar wij wijzen degene die de verantwoordelijkheid draagt erop om maatregelen te nemen.

De **voorzitter**: Er zijn geen aanvullende vragen meer. Wij komen nu tot de afsluiting van dit algemeen overleg cyber security. Ik zal de toezeggingen voorlezen, waarbij de Minister zal aangeven of ze ook als zodanig zijn gedaan door hem.
– De leden van de commissie V en J ontvangen een uitnodiging voor de Global Conference on Cyberspace in april 2015.

Minister **Opstelten**: Op 16 en 17 april.

De **voorzitter**: Dat zijn waarschijnlijk ook echt vip-uitnodigingen?

Minister **Opstelten**: Aan de leden van de Staten-Generaal.

De **voorzitter**: Dat is nog mooier, want ik ben zelf tijdelijk lid van deze commissie, dus dan krijgen de leden van de Staten-Generaal alle 150 een uitnodiging voor de Global Conference on Cyberspace. Je moet natuurlijk toch ook aan de 1.300 mensen komen.

Minister **Opstelten**: Er wordt een tentje bij gezet!

De **voorzitter**: Ik vervolg met de andere toezeggingen.
– de Minister neemt informatie over de voortgang van de ontwikkeling van een systeem van certificering, naar voorbeeld van het Verenigd Koninkrijk, mee in de voortgangsbrief cyber security die de Kamer aan het einde van het jaar ontvangt.
– de Kamer ontvangt nadere informatie over de koppeling van databestanden en, indien mogelijk, een overzicht van de bestaande koppelingen voor het AO Dataretentie en privacy op 26 maart van dit jaar. De Minister doet daartoe een poging en komt er schriftelijk op terug.
– de Kamer ontvangt binnen twee weken een brief over de voortgang van het Landelijk Meldpunt Internetoplichting en Europese veiligheidseisen.

Minister **Opstelten**: Brusselse veiligheidseisen.

De **voorzitter**: Dan zijn daarmee de toezeggingen juist genoteerd, zijn alle vragen beantwoord en kunnen wij naar het eind van dit algemeen overleg. Ik dank iedereen voor zijn inzet, ik dank uiteraard de Minister en zijn ambtenaren, de aanwezigen en de collega's.

Sluiting 15.55 uur.